

AK

**Notice of Allowability**

Application No.

10/058,212

Examiner

Kaveh Abrishamkar

Applicant(s)

LAMBERT, ROBERT J.

Art Unit

2131

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the Request for Continued Examination (RCE) filed on 10/30/2007.
2. ☒ The allowed claim(s) is/are 1 and 3-10.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All    b) ☐ Some\*    c) ☐ None    of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.

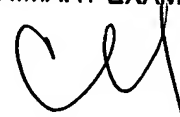
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material

5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date 11/7/08
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

**CHRISTOPHER REVAK  
PRIMARY EXAMINER**



### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brett Slaney on January 7, 2008.

The application has been amended as follows:

1. (currently amended) A method of adding elements of a finite field comprising the steps of:
  - a) storing a first element and a second element in respective ones of a pair of registers, each of said pair of registers comprising a first predetermined number of machine words;
  - b) establishing an accumulator having a second predetermined number of machine words;
  - c) performing a non-reducing computation of the corresponding machine words representing each of said first and second elements by taking the exclusive-or of said first and second elements to obtain, in said accumulator, a representation of a unreduced result of the addition of said elements, and, upon computing said unreduced result:

d) performing a specific modular reduction of said unreduced result to reduce said unreduced result to that of a field element of said finite field to obtain a reduced result[[.]]; and

e) using said reduced result in a cryptographic operation.

4. (currently amended) A method of performing a finite field operation on elements of a finite field, comprising the steps of:

a) representing each element as a predetermined number of machine words;  
b) performing a non-reducing wordsized operation on said representations, said wordsized operation corresponding to said finite field operation;

c) completing said non-reducing wordsized operation for each word of said representations to obtain an unreduced result; [[and]]

d) upon computing said unreduced result, performing a specific modular reduction of said unreduced result to reduce said unreduced result to that of a field element of said finite field to obtain a reduced result[[.]]; and

e) using said reduced result in a cryptographic operation.

6. (currently amended) A cryptographic system comprising:

a) a plurality of elliptic curves, each specifying elliptic curve parameters and a respective finite field;

b) a plurality of finite field settings corresponding to each finite field;

- c) a plurality of wordsized finite fields, each having routines, each finite field being assigned to one of said wordsized finite fields;
- d) a reduction routine for each finite field;
- e) a processor computational apparatus configured to perform a cryptographic operation by the steps of:
  - i) selecting one of said elliptic curves; and
  - ii) performing a non-reducing cryptographic function using the routines from the wordsized finite field to which the respective finite field corresponding to said selected elliptic curve is assigned to obtain an unreduced result; said routines including at least one finite field operation and, upon obtaining said unreduced result, performing a modular reduction according to said respective finite field to reduce said unreduced result to that of a field element of said respective finite field to obtain a reduced result of said operation in a predetermined number of words.

### REASONS FOR ALLOWANCE

Claims 1 and 3-10 are allowed.

The following is an examiner's statement of reasons for allowance:

The aforementioned claims are allowable over the Cited Prior Art (CPA), Dworkin et al. (U.S. Patent 6,230,179), because the CPA does not teach nor suggest all of limitations of currently amended claims 1, and 3-6, and the subsequent dependent claims.

The CPA fails to disclose performing finite field operations by performing non-reducing computations and then a reduction at the end. Dworkin performs reduction at each step, and does not just perform on reduction at the end.

This method of performing finite field operations is in improvement of the prior arts because this method increases randomness and inhibits side channel attacks.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number:  
10/058,212  
Art Unit: 2131

Page 6

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA 1108108  
KA  
01/08/2008

CHRISTOPHER REVAK  
PRIMARY EXAMINER

